



Privacy Impact Assessment

Consumer Complaint Monitoring System II (CCMS II)

***Food Safety and Inspection Service
(FSIS)***

Date: November 2009

Revision: 1.0



Document Information

Owner Details	
Name	Robert Teclaw
Contact Number	(202) 690-6045
E-mail Address	robert.teclaw@fsis.usda.gov

Revision History			
Revision	Date	Author	Comments
1.0	October 2009	Sam Gupta	Initial draft
2.0	October 2009	Sam Gupta	Update based on the privacy officer's comment.

Distribution List			
Name	Title	Agency/Office	Contact Information



Table of Contents

DOCUMENT INFORMATION	II
TABLE OF CONTENTS.....	III
1 SYSTEM INFORMATION.....	1
2 DATA INFORMATION	2
2.1 Data Collection	2
2.2 Data Use	3
2.3 Data Retention.....	6
2.4 Data Sharing.....	6
2.5 Data Access	7
2.6 Customer Protection	9
3 SYSTEM OF RECORD	10
4 TECHNOLOGY	10
5 COMPLETION INSTRUCTIONS.....	12

1 System Information

System Information	
Agency:	USDA/FSIS/OPHS
System Name:	Consumer Complaint Monitoring System II
System Type:	<input checked="" type="checkbox"/> Major Application <input type="checkbox"/> General Support System <input type="checkbox"/> Non-major Application
System Categorization (per FIPS 199):	<input type="checkbox"/> High <input checked="" type="checkbox"/> Moderate <input type="checkbox"/> Low
Description of System:	<p>The primary goal of Consumer Complaint Management System (CCMS) is to support and augment Office of Public Health Science analysts in their ability to rapidly identify consumer health risks associated with FSIS regulated products. It is designed to respond quickly and effectively to <i>characterize possible threats to FSIS regulated products</i>. The CCMS database is a relational database of complaints about food products and food-borne illnesses that FSIS developed.</p> <p>CCMS will help OPHS identify and evaluate potential food-borne hazards, determine estimates of risk to human health, and respond to recognized, emerging, or potential threats to the food supply. The database must collect enough information to assist FSIS with trace-back or trace forward investigations to identify product disposition and/or the origin of hazards. This information will be used to coordinate the recall of products when required.</p> <p>CCMS is designed to be flexible and expandable for future integration with other Federal Departments and Agencies, other USDA Agencies, State Governments, and food safety and public health related associations.</p>
Who owns this system? (Name, agency, contact information)	Robert Teclaw USDA/FSIS/OPHS 202-690-6045 robert.teclaw@fsis.usda.gov
Who is the security contact for this system? (Name, agency, contact information)	Olukayode Adeyosoye USDA/FSIS/OPEER/OCIO/OCTO/ISSP 202-418-8813 olukayode.adeyosoye@fsis.usda.gov
Who completed this document? (Name, agency, contact information)	Sam Gupta Project Manager InfoReliance Corporation 703.246.9360 ext. 562 sam.gupta@info reliance.com

2 Data Information

2.1 Data Collection

No.	Question	Response
1	Generally describe the data to be used in the system.	Consumer complaints information.
2	Does the system collect Social Security Numbers (SSNs) or Taxpayer Identification Numbers (TINs)?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No – If NO, go to question 3.
2.1	State the law or regulation that requires the collection of this information.	
3	Is the use of the data both relevant and necessary to the purpose for which the system is being designed? In other words, the data is absolutely needed and has significant and demonstrable bearing on the system's purpose as required by statute or by Executive order of the President.	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
4	Sources of the data in the system.	Manual data entry, received from consumers directly through 1-800 number. CCMS II exposes a web service. This facilitates an import function.
4.1	What data is being collected from the customer?	First Name, Last Name, Address, Phone number, email address, details of the complaint.
4.2	What USDA agencies are providing data for use in the system?	FSIS
4.3	What state and local agencies are providing data for use in the system?	N/A
4.4	From what other third party sources is data being collected?	N/A
5	Will data be collected from sources outside your agency? For example, customers, USDA sources (i.e., NFC, RD, etc.) or Non-USDA sources.	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No – If NO, go to question 6. Information will be collected from consumers directly through USDA / FSIS employees. There is also a feed from the HOTLINE system into CCMS II.
5.1	How will the data collected from customers be verified for accuracy, relevance, timeliness, and completeness?	Collected by trained analyst while speaking or interacting directly with the consumer.

No.	Question	Response
5.2	How will the data collected from USDA sources be verified for accuracy, relevance, timeliness, and completeness?	Collected by trained analyst while speaking or interacting directly with the consumer. Customers of FSIS bear the 'burden of proof' with respect to the accuracy and completeness as well as with respect to the type of correction they provide. The Food Safety and Inspection Service may be unable to process, in a timely fashion or at all if customers omit one or more of the requested elements. FSIS will maintain the integrity of privacy related information and comply with the statutory requirements to protect the information it gathers and disseminates. These include the Privacy Act of 1974, as amended, the Paperwork Reduction Act of 1995, the Computer Security Act of 1987, the Freedom of Information Act, and OMB Circulars A-123, A-127, and A-130.
5.3	How will the data collected from non-USDA sources be verified for accuracy, relevance, timeliness, and completeness?	N/A

2.2 Data Use

No.	Question	Response
6	Individuals must be informed in writing of the principal purpose of the information being collected from them. What is the principal purpose of the data being collected?	The information provided by the customer will be used to assist in identifying the general consumer health risks throughout the United States.
7	Will the data be used for any other purpose?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No – If NO, go to question 8.
7.1	What are the other purposes?	
8	Is the use of the data both relevant and necessary to the purpose for which the system is being designed? In other words, the data is absolutely needed and has significant and demonstrable bearing on the system's purpose as required by statute or by Executive order of the President	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No US Code TITLE 7, CHAPTER 55 - 2204 states that the Secretary of Agriculture may conduct any survey or other information collection, and employ any sampling or other statistical method, that the Secretary determines is appropriate.
9	Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected (i.e., aggregating farm loans by zip codes in which only one farm exists.)?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No – If NO, go to question 10.
9.1	Will the new data be placed in the individual's record (customer or employee)?	<input type="checkbox"/> Yes <input type="checkbox"/> No



Privacy Impact Assessment for CCMS II

No.	Question	Response
9.2	Can the system make determinations about customers or employees that would not be possible without the new data?	<input type="checkbox"/> Yes <input type="checkbox"/> No
9.3	How will the new data be verified for relevance and accuracy?	
10	Individuals must be informed in writing of the routine uses of the information being collected from them. What are the intended routine uses of the data being collected?	<p>The information provided will be used to identify consumer health risks.</p> <p>Routine use for disclosure to the Department of Justice for use in litigation, for disclosure to adjudicative body in litigation, law enforcement purposes, for disclosure to a Member of Congress at the request of a constituent, for disclosure to the National Archives and Records Administration or to the General Services Administration for records management inspections conducted under 44 USC 2904 and 2906, for disclosure to FSIS contractors pursuant to 5 USC 552a(m), for disclosure to appropriate agencies, entities, and persons when the agency suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised.</p> <p>USDA will disclose information about individuals from this system of records in accordance with the Federal Funding Accountability and Transparency Act of 2006 (Pub. L. No. 109-282; codified at 31 U.S.C. 6101, et seq.); section 204 of the E-Government Act of 2002 (Pub. L. No. 107B347; 44 U.S.C. 3501 note), and the Office of Federal Procurement Policy Act (41 U.S.C. 403 et seq.), or similar statutes requiring agencies to make available information concerning Federal financial assistance, including grants, subgrants, loan awards, cooperative agreements and other financial assistance; and contracts, subcontracts, purchase orders, task orders, and delivery orders.</p>
11	Will the data be used for any other uses (routine or otherwise)?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No – If NO, go to question 12.
11.1	What are the other uses?	

No.	Question	Response
12	Automation of systems can lead to the consolidation of data – bringing data from multiple sources into one central location/system – and consolidation of administrative controls. When administrative controls are consolidated, they should be evaluated so that all necessary privacy controls remain in place to the degree necessary to continue to control access to and use of the data. Is data being consolidated?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
12.1	What controls are in place to protect the data and prevent unauthorized access?	<p>There are Firewalls and other security precautions, for example, all authorized staff <i>using the system must comply with the Agency's general use policy for information technology. Rules of behavior and consequences, and system use notifications are in accordance with the Privacy Act (subsection e [9]) and OMB Circular A-130, Appendix III. The security controls in the system are reviewed when significant modifications are made to the system, but at least every three years. Active Directory and CCMS II role based security is used to identify the Tracker user as authorized for access and as having a restricted set up responsibilities and capabilities with in the system. When the user initiates the system, their secure network login credentials are passed to the system via Active Directory.</i></p> <p>By having a Department of Agriculture email account, their network login credentials are checked against authorized system user role membership and access privileges are restricted accordingly. FSIS system users must pass a government background check prior to having system access.</p> <p><i>Authorized user login identifiers are appended to any system records created or updated, along with the date and time of the record creation or change. This allows administrators to identify the source of any incorrect or incomplete data as recorded in the system. Contractors authorized to access the system are governed by contracts identifying rules of behavior for Department of Agriculture and FSIS systems and security. Contracts are reviewed upon renewal by management and contract personnel expert in such matters.</i></p>
13	Are processes being consolidated?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No – If NO, go to question 14.
13.1	What controls are in place to protect the data and prevent unauthorized access?	

2.3 Data Retention

No.	Question	Response
14	Is the data periodically purged from the system?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No – If NO, go to question 15.
14.1	How long is the data retained whether it is on paper, electronic, in the system or in a backup?	N/A
14.2	What are the procedures for purging the data at the end of the retention period?	N/A
14.3	Where are these procedures documented?	N/A
15	While the data is retained in the system, what are the requirements for determining if the data is still sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations?	There are no requirements.
16	Is the data retained in the system the minimum necessary for the proper performance of a documented agency function?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No These records will be maintained until they become inactive, at which time they will be destroyed or retired in accordance with the Department's published records disposition schedules, as approved by the National Archives and Records Administration (NARA). FSIS keeps accurate accounts of when and to whom it has disclosed personal records. This includes contact information for the person or agency that requested the personal records. These accounts are to be kept for five years, or the lifetime of the record, whichever is longer. Unless the records were shared for law enforcement purposes, the accounts of the disclosures should be available to the data subject upon request.

2.4 Data Sharing

No.	Question	Response
17	Will other agencies share data or have access to data in this system (i.e., international, federal, state, local, other, etc.)?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No – If NO, go to question 18.
17.1	How will the data be used by the other agency?	
17.2	Who is responsible for assuring the other agency properly uses the data?	
18	Is the data transmitted to another agency or an independent site?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No – If NO, go to question 19.

No.	Question	Response
18.1	Is there appropriate agreement in place to document the interconnection and ensure the PII and/or Privacy Act data is appropriately protected?	
19	Is the system operated in more than one site?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No – If NO, go to question 20.
19.1	How will consistent use of the system and data be maintained in all sites?	

2.5 Data Access

No.	Question	Response
20	Who will have access to the data in the system (i.e., users, managers, system administrators, developers, etc.)?	System Administrators and users of the system will have access. Authorized employees are assigned level-of-access roles based on their job functions. Roles limit the update and printing capabilities to those deemed necessary for specified job functions. Multiple levels of access exist based on the authorized user's role and job function. The level of access for the user restricts the data that may be seen and the degree to which data may be modified by the user.
21	How will user access to the data be determined?	Access is determined by the business owners and system administrator.
21.1	Are criteria, procedures, controls, and responsibilities regarding user access documented?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No To gain access to the CCMS II system, a user must have 1) an account on the FSIS Active Directory; and 2) have a role within the CCMS II application.

No.	Question	Response
22	How will user access to the data be restricted?	<p>Role based security is implemented throughout the system. All authorized staff using the system must comply with the Agency's general use policy for information technology. Rules of behavior and consequences, and system use notifications are in accordance with the Privacy Act (subsection e [9]) and OMB Circular A-130, Appendix III. The security controls in the system are reviewed when significant modifications are made to the system, but at least every three years.</p> <p>Active Directory and CCMS II role based security is used to identify the Tracker user as authorized for access and as having a restricted set of responsibilities and capabilities within the system. When the user initiates the system, their secure network login credentials are passed to the system via Active Directory.</p> <p>By having a Department of Agriculture email account, their network login credentials are checked against authorized system user role membership and access privileges are restricted accordingly. FSIS system users must pass a government background check prior to having system access.</p> <p>Annual, recurring security training is practiced and conducted through the Office of the Chief Information Officer. Authorized user login identifiers are appended to any system records created or updated, along with the date and time of the record creation or change.</p> <p>This allows administrators to identify the source of any incorrect or incomplete data as recorded in the system. Contractors authorized to access the system are governed by contracts identifying rules of behavior for Department of Agriculture and FSIS systems and security. Contracts are reviewed upon renewal by management and contract personnel expert in such matters.</p>
22.1	Are procedures in place to detect or deter browsing or unauthorized user access?	<p><input checked="" type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>An access agreement describes prohibited activities such as browsing. Activity by authorized users is monitored, logged, and audited. All users are required to undergo Department-approved computer security awareness training prior to access and must complete computer security training yearly in order to retain access.</p>



Privacy Impact Assessment for CCMS II

No.	Question	Response
23	Does the system employ security controls to make information unusable to unauthorized individuals (i.e., encryption, strong authentication procedures, etc.)?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No

2.6 Customer Protection

No.	Question	Response
24	Who will be responsible for protecting the privacy rights of the customers and employees affected by the interface (i.e., office, person, departmental position, etc.)?	USDA FSIS OCIO Security
25	How can customers and employees contact the office or person responsible for protecting their privacy rights?	<p>Employees must e-mail the system owner to inquire about data in the system. Public individuals who have reason to believe that this system might have records pertaining to them should write to the FSIS FOIA Officer at:</p> <p>FSIS Freedom of Information Act Office, Room 1140, 1400 Independence Avenue, SW Washington, DC 20250-3700 Phone: (202) 690-3882 Fax (202) 690-3023 Email: fsis.foia@usda.gov.</p> <p>The individual must specify that he or she wishes the records of the system to be checked. At a minimum, the individual should include: name; date and place of birth; current mailing address and zip code; signature; a brief description of the circumstances that caused the creation of the record (including the city and/or country and the approximate dates) which gives the individual cause to believe that this system has records pertaining to him or her.</p>
26	A "breach" refers to a situation where data and/or information assets are unduly exposed. Is a breach notification policy in place for this system?	<input checked="" type="checkbox"/> Yes – If YES, go to question 27. <input type="checkbox"/> No The System Contingency Plan will address incident response, and will refer to FSIS policy for Incident Handling.
26.1	If NO, please enter the Plan of Action and Milestones (POA&M) number with the estimated completion date.	

No.	Question	Response
27	Consider the following: <ul style="list-style-type: none"> Consolidation and linkage of files and systems Derivation of data Accelerated information processing and decision making Use of new technologies Is there a potential to deprive a customer of due process rights (fundamental rules of fairness)?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No – If NO, go to question 28.
27.1	Explain how this will be mitigated?	
28	How will the system and its use ensure equitable treatment of customers?	N/A
29	Is there any possibility of treating customers or employees differently based upon their individual or group characteristics?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No – If NO, go to question 30
29.1	Explain	

3 System of Record

No.	Question	Response
30	Can the data be retrieved by a personal identifier? In other words, does the system actually retrieve data by the name of an individual or by some other unique number, symbol, or identifying attribute of the individual?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No – If NO, go to question 31
30.1	How will the data be retrieved? In other words, what is the identifying attribute (i.e., employee number, social security number, etc.)?	First Name, Last Name, Address, Phone number, email address, details of the complaint are collected.
30.2	Under which Systems of Record (SOR) notice does the system operate? Provide number, name and publication date. (SORs can be viewed at www.access.GPO.gov .)	A new SORN will need to be created. Once the PIA is approved. The SORN process will begin.
30.3	If the system is being modified, will the SOR require amendment or revision?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No

4 Technology

No.	Question	Response
31	Is the system using technologies in ways not previously employed by the agency (e.g., Caller-ID)?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No – If NO, the questionnaire is complete.



Privacy Impact Assessment for CCMS II

No.	Question	Response
31.1	How does the use of this technology affect customer privacy?	



5 Completion Instructions

Upon completion of this Privacy Impact Assessment for this system, the answer to OMB A-11, Planning, Budgeting, Acquisition and Management of Capital Assets, Part 7, Section E, Question 8c is:

1. Yes.

PLEASE SUBMIT A COPY TO THE OFFICE OF THE ASSOCIATE CHIEF
INFORMATION OFFICE FOR CYBER SECURITY.



Privacy Impact Assessment Authorization

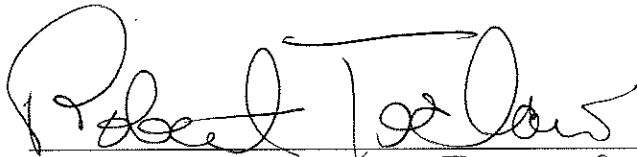
Memorandum

I have carefully assessed the Privacy Impact Assessment for the

Consumer Complaint Monitoring System II (*CCMS II*)

This document has been completed in accordance with the requirements of the E-Government Act of 2002.

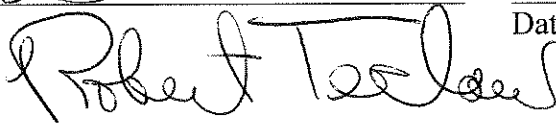
We fully accept the changes as needed improvements and authorize initiation of work to proceed. Based on our authority and judgment, the continued operation of this system is authorized.



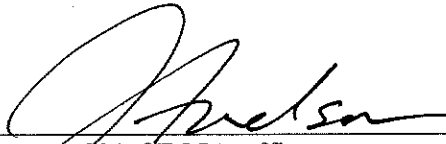
System Manager/Owner
OR Project Representative
OR Program/Office Head.

11/17/09

Date



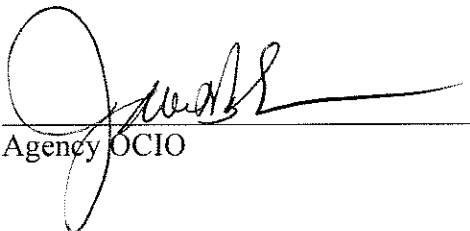
11/17/09



Agency's Chief FOIA officer
OR Senior Official for Privacy
OR Designated privacy person

11/30/09

Date



Agency OCIO

12/17/09

Date